

David M. Berger (SBN 277526)

GIBBS LAW GROUP LLP

1111 Broadway, Suite 2100

Oakland, California 94607

Telephone: (510) 350-9713

Facsimile: (510) 350-9701

dmb@classlawgroup.com

Norman E. Siegel (*pro hac vice*)

J. Austin Moore (*pro hac vice*)

Kasey Youngentob (*pro hac vice*)

STUEVE SIEGEL HANSON LLP

460 Nichols Road, Suite 200

Kansas City, Missouri 64112

(816) 714-7100 (tel.)

siegel@stuevesiegel.com

moore@stuevesiegel.com

youngentob@stuevesiegel.com

**UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA**

ABBY LINEBERRY, TERRY MICHAEL
COOK and MIGUEL CORDERO, individually
and on behalf of all others similarly situated,

Plaintiffs,

vs.

ADDSHOPPERS, INC., and PEET'S COFFEE,
INC.,

Defendants.

Case No. 3:23-cv-01996-VC

**PLAINTIFFS' CONSOLIDATED
RESPONSE IN OPPOSITION TO
DEFENDANTS' MOTIONS
TO DISMISS**

Judge: Hon. Vince Chhabria

Hearing: January 23, 2025

Time: 10:00 a.m.

Courtroom: 4

TABLE OF CONTENTS

TABLE OF AUTHORITIES	ii
I. INTRODUCTION	1
II. FACTUAL BACKGROUND	2
III. ARGUMENT	7
A. Legal Standards.....	7
1. Motion to Dismiss.....	7
2. Law of the Case	7
B. Plaintiffs have standing to pursue all their claims.	7
1. The law of the case doctrine bars re-litigation of these issues.....	8
2. Even if not barred, Defendants’ standing arguments are not persuasive....	9
3. Plaintiff Coredero has Article III standing.....	9
4. Plaintiff Lineberry has Article III standing.....	11
C. Plaintiffs have sufficiently pleaded their statutory claims.	12
1. The Court has already rejected Peet’s argument that non-California representatives cannot assert claims against California companies.....	12
2. The Court has already decided that Plaintiffs sufficiently allege the elements of CIPA.	13
3. Defendants’ recycled CDAFA arguments should again be rejected.	14
IV. CONCLUSION.....	15

TABLE OF AUTHORITIES

Cases

<i>Ashcroft v. Iqbal</i> , 556 U.S. 662 (2009).....	7
<i>Balanzar v. Fidelity Brokerage Services, LLC</i> , --- F.Supp.3d ---, 2023 WL 1767011 (S.D. Cal. Feb. 3, 2023).....	13
<i>Brown v. Google LLC</i> , 685 F. Supp. 3d 909 (N.D. Cal. 2023).....	5, 15
<i>Byars v. Sterling Jewelers, Inc.</i> , 2023 WL 2996686 (C.D. Cal. Apr. 5, 2023)	8
<i>Carrese v. Yes Online Inc.</i> , 2016 WL 6069198 (C.D. Cal. Oct. 13, 2016).....	12
<i>Chavez v. Bank of Am. Corp.</i> , 2012 WL 1594272 (N.D. Cal. May 4, 2012)	7, 9
<i>Christianson v. Colt Indus. Operating Corp.</i> , 486 U.S. 800 (1988).....	7
<i>Frasco v. Flo Health, Inc.</i> , 2024 WL 4280933 (N.D. Cal. Sept. 23, 2024)	15
<i>Hanna Boys Ctr. v. Miller</i> , 853 F.2d 682 (9th Cir. 1988)	7
<i>Hazel v. Prudential Fin., Inc.</i> , 2023 WL 3933073 (N.D. Cal. June 9, 2023)	13
<i>In re Benny</i> , 81 F.3d 91 (9th Cir. 1996)	7
<i>In re Facebook, Inc. Internet Tracking Litig. (Facebook Tracking)</i> , 956 F.3d 589 (9th Cir. 2020)	8, 11, 13
<i>In re Facebook, Inc., Consumer Privacy Litig.</i> , 402 F. Supp. 3d 767 (N.D. Cal. Sept. 2019).....	8
<i>Ingrao v. AddShoppers, Inc.</i> , 2024 WL 4892514 (E.D. Pa. Nov. 25, 2024)	9
<i>Lightoller v. Jetblue Airways, Corp.</i> , 2023 WL 3963823 (S.D. Cal. June 12, 2023).....	8

<i>Mata v. Zillow Grp., Inc.</i> , 2024 WL 5161955 (S.D. Cal. Dec. 18, 2024).....	14
<i>Rodriguez v. Google LLC</i> , 2024 WL 38302 (N.D. Cal. Jan. 3, 2024)	15
<i>Safe Air for Everyone v. Meyer</i> , <i>et al.</i> , 373 F.3d 1035 (9th Cir. 2004)	7
<i>Spokeo, Inc. v. Robins</i> , 578 U.S. 330 (2016).....	8
<i>Thomas v. Bible</i> , 983 F.2d 152 (9th Cir. 1993)	7
<i>Torres v. Prudential Fin., Inc.</i> , 2024 WL 4894289 (N.D. Cal. Nov. 26, 2024)	13
<i>TransUnion LLC v. Ramirez</i> , 594 U.S. 413 (2021).....	8
<i>United States v. Caputo</i> , 2019 WL 5788305 (D. Or. Nov. 6, 2019).....	12
<i>United States v. Christensen</i> , 828 F.3d 763 (9th Cir. 2015)	5
<i>United States v. Greiner</i> , 235 F. App'x 541 (9th Cir. 2007)	12
<i>United States v. Heckenkamp</i> , 482 F.3d 1142 (9th Cir. 2007)	12
<i>Yoon v. Meta Platforms, Inc.</i> , 2024 WL 5264041 (N.D. Cal. Dec. 30, 2024).....	14
Statutes	
California Penal Code § 631	5, 11, 14
Cal. Civ. Code § 1798.110.....	10
Other Authorities	
18 Charles Alan Wright et al., Federal Practice and Procedure § 4478, at 790 (1981)	7

I. INTRODUCTION

AddShoppers, Inc. and Peet's Coffee, Inc. refuse to accept this Court's prior rulings. Cloaked as challenges to the First Amended Complaint, Defendants advance arguments identical to those the Court has already considered and rejected, including challenges to Article III standing and the sufficiency of Plaintiffs' claims under the California Invasion of Privacy Act (CIPA) and the Computer Data Access and Fraud Act (CDAFA).

These issues were already decided. After extensive briefing and argument, the Court held that Plaintiffs sufficiently alleged Article III standing based on Defendants' unauthorized interception of individuals' browsing data and misuse of that data to send targeted emails. When Peet's again challenged standing in opposing the Amended Complaint as futile, the Court rejected that challenge by allowing the claims to proceed. The Court further concluded that Plaintiffs adequately alleged CIPA violations by demonstrating that AddShoppers' tracking cookies intercepted communications "in transit" and unauthorized access and use of their information under CDAFA. Yet Defendants now seek to relitigate the same points.

Peet's once again asserts that Plaintiff Terry Cook cannot state a CIPA claim because he does not allege that an interception occurred in California—an argument the Court dismissed as "too weak or undeveloped to merit a response." Dkt. 89 at 5. AddShoppers likewise rehashes its assertion that Plaintiffs fail to allege the elements of a CIPA claim, reasserting arguments the Court specifically considered and rejected. Defendants also revive their CDAFA argument, insisting that Plaintiffs fail to allege a cognizable economic injury—another assertion this Court has rejected.

The law of the case doctrine bars Defendants from relitigating these settled issues. The Court's prior rulings remain binding absent new evidence, a change in controlling law, or clear error, none of which Defendants have identified. The amendments in the First Amended Complaint do not alter the core analysis underpinning the Court's prior rulings, and Defendants' motions simply repackage previously rejected arguments. The Court should deny Defendants' motions in their entirety.

II. FACTUAL BACKGROUND

This case was filed in April 2023. *See* Dkt. 1 (“Compl.”). The Complaint alleges that AddShoppers operates an unlawful marketing scheme through its “SafeOpt” program, which illicitly tracks individuals’ internet activity, collects their personal information without consent, and uses that data for targeted solicitations. *Id.* ¶¶ 1–2. AddShoppers markets SafeOpt as a consumer-friendly service providing exclusive offers. *Id.* ¶ 3. But in reality, individuals are unwittingly enrolled into the program when they make purchases on websites that are part of AddShoppers’ “Data Co-Op.” *Id.* Companies that join the co-op agree to install AddShoppers’ JavaScript code on their websites. *Id.* ¶ 38. When an internet user creates an account or makes a purchase with the business, AddShoppers surreptitiously places a third-party tracking cookie on the user’s browser. *Id.* That cookie contains a unique identifier, which AddShoppers associates with the user’s personal information. *Id.* With the hidden tracking cookie in place, AddShoppers can monitor the individual’s browsing activity across the internet. *Id.* ¶ 39. If the user visits another website within the SafeOpt network, the cookie values “sync” and AddShoppers tracks the individual’s activity on the website, including the exact URL and products the user views. *Id.*

Thus, even when individuals leave a website without providing any personal information, AddShoppers can still identify them, track their online browsing activity, and send them direct unsolicited email promotions. *Id.* The Complaint cites numerous examples of consumers complaining about receiving targeted emails from retailers “via SafeOpt,” despite never providing their personal information to those retailers. *Id.* ¶ 4; *see also id.* ¶¶ 45–51. Consumers described the practice as “creepy,” “sleazy,” “disgusting advertising,” “unethical,” and an “invasion of privacy.” *Id.* ¶ 4; *see also id.* ¶ 45. Some report receiving emails even after trying to opt out of the network. *Id.* ¶ 50.

As a result, Plaintiffs brought this class action against AddShoppers; two members of AddShoppers’ data co-op, Presidio Brands, Inc. (doing business as Every Man Jack) and Peet’s Coffee, Inc. (together, retailer defendants); and other unknown John Doe companies that

participated in the co-op. *Id.* ¶¶ 11-13. Plaintiffs asserted nine causes of action, including violations of CIPA and CDAFA, statutory larceny, unfair competition, trespass to chattels, unjust enrichment, and common law invasion of privacy. *Id.* ¶¶ 88-170.

AddShoppers and the retailer defendants each moved to dismiss on June 20, 2023. *See* Dkts. 50, 51. All defendants argued that:

- Plaintiffs lacked Article III standing for various reasons, including because they did not voluntarily share personal information with the retailer defendants and failed to allege facts showing the disclosure of confidential or private information. *See* Dkt. 50 at 14-15; Dkt. 51 at 13-15.
- Plaintiffs' CIPA claims failed because the cookie banners on the retailer defendants' website ostensibly provided consent to the practices. *See* Dkt. 50 at 22; Dkt. 51 at 16-20.
- Plaintiffs' CDAFA claims failed because they did not show that AddShoppers acted "without permission," which purportedly requires a showing that it accessed their personal information by circumventing technical or code-based barriers designed to prevent such access. *See* Dkt. 50 at 18-19; Dkt. 51 at 23.

AddShoppers further argued that:

- The Court lacked personal jurisdiction over the company. *See* Dkt. 50 at 12-14.
- The Court should interpret wiretapping narrowly under the "rule of lenity" because other federal and state statutory regimes purportedly permit AddShoppers to email and collect and share information about consumers without their consent. *See id.* at 15-17.
- CIPA does not apply to the allegations, but even if it did, Plaintiffs failed to adequately allege the "in transit" element under CIPA. *See id.* at 18.
- Plaintiffs failed to allege damages under CDAFA. *See id.* at 20.

Similarly, the retailer defendants argued that:

- The CIPA claims failed because Plaintiffs do not reside in California and their communications were not intercepted in California. *See* Dkt. 51 at 13-15, 21-22.
- The CIPA claim failed because Plaintiffs did not disclose confidential information to the retailer defendants. *See id.* at 22-23.

Those motions were fully briefed and then argued on October 5, 2023. *See* Dkt. 67.

On January 17, 2024, the Court granted in part and denied in part both motions to dismiss. *See* Dkt. 89. Specifically, the Court upheld specific personal jurisdiction over AddShoppers in California, concluding that AddShoppers’ contracts with California retailers directly facilitated the alleged harm—intercepting consumers’ data and using it to send unsolicited emails. *Id.* at 1-2. Unlike cases where contractual arrangements were unrelated to the alleged harm, here AddShoppers’ agreements were integral to its data collection and outreach scheme. *See id.*

The Court also held that Plaintiffs sufficiently alleged Article III standing against both AddShoppers and the retailer defendants. *Id.* at 2. It reasoned that “[m]isappropriating a person’s browsing activity across a network of thousands of online retailers and using it to barrage that person’s devices with unwanted email communications—particularly without providing a way to opt out—is the type of privacy intrusion that federal courts can address.” *Id.* (collecting cases).

The Court determined that Plaintiffs “clearly ha[d] alleged standing to sue AddShoppers,” as the company “orchestrated the scheme and then directly took the injury-causing actions.” *Id.* For the retailer defendants, standing was a “close[r] question,” but their knowing participation in the scheme—joining AddShoppers’ network and facilitating the systematic aggregation and misuse of consumers’ browsing data—was integral to the alleged harm. *Id.* The Court noted that the injury arose not from a single unwanted email but from the extensive aggregation and misuse of personal information across thousands of retail sites, a process the retailers knowingly supported. *Id.* at 2-3. This level of involvement was sufficient to establish standing against the retailers in federal court. *See id.*

The Court also held that the Complaint adequately alleged statutory standing for the claims against AddShoppers and under the UCL, CDAFA, and for statutory larceny, each of which requires an allegation of monetary loss. *Id.* at 3. The Court noted that the Complaint created a reasonable inference that Plaintiffs purchased products from retailers within AddShoppers’ network and, as a result, entered the network and received unwanted email communications. *Id.* at 4. The Complaint also “allege[d] clearly” that Plaintiffs would not have made those purchases had they known doing so would subject them to the alleged scheme. *Id.*

The Court rejected Defendants’ consent defense. *Id.* at 4-5. It concluded that neither the Complaint nor the motion-to-dismiss materials considered “establish[ed] that the plaintiffs consented to the alleged misappropriation of their data or the subsequent emails.” *Id.*

As for the CIPA claims, the Court held that “[P]laintiffs sufficiently allege[d] that the communications were intercepted ‘in transit’ within the meaning of [California Penal Code] § 631(a).” *Id.* at 5. The Court noted that the Complaint didn’t just parrot statutory language; it described in detail “how AddShoppers’s cookies intercept the information in real time, and it point[ed] to statements allegedly made by AddShoppers about real time transmission.” *Id.*¹ The Court dismissed Defendants’ other arguments against the CIPA claims as “too weak or undeveloped to merit a response.” *Id.*

As for the CDAFA claims, the Court held, consistent with Ninth Circuit precedent, that CDAFA does not require unauthorized access to information via a “technical circumvention,” but rather the unauthorized taking and using of such information. *Id.* at 6 (citing *United States v. Christensen*, 828 F.3d 763, 789 (9th Cir. 2015); *Brown v. Google LLC*, 685 F. Supp. 3d 909, 940 n.38 (N.D. Cal. 2023)). The Court concluded that plaintiffs sufficiently alleged unauthorized taking and use of their information. *See id.*

The Court dismissed Plaintiffs’ claims for statutory larceny, trespass to chattels, unjust enrichment, and invasion of privacy, as well as the claims against the John Doe defendants. *See id.* at 6-8. While the Court allowed Plaintiffs the opportunity to amend, they chose to proceed on the surviving claims. AddShoppers then filed a motion for leave to appeal the motion to dismiss order, *see* Dkt. 100, which the Court denied, *see* Dkt. 110.

On October 22, 2024, Plaintiffs moved for leave to file a First Amended Complaint. *See* Dkt. 121. The proposed Amended Complaint included the same substantive allegations as the

¹ The Court dismissed Plaintiff Dessart’s CIPA claim against Presidio Brands because Dessart’s wife was the one who interacted with Every Man Jack’s website. *See* Dkt. 89 at 5-6. Dessart later settled his claims in an individual pre-certification settlement approved by the Court. *See* Dkts. 122-124.

original complaint and modified it only to add Miguel Cordero as a named plaintiff, remove Plaintiff Oather McClung (who voluntarily dismissed his claims), and remove the dismissed Doe defendants.² *See* Dkt. 121-3. Both Peet’s and AddShoppers opposed the amendment. *See* Dkts. 126, 127.

AddShoppers focused its opposition on supposed delays and prejudice it would suffer from an amendment. *See* Dkt. 126 at 6-11. Peet’s, for its part, asserted that the proposed amendment was futile, arguing that Cordero’s factual allegations were insufficient to establish standing or state a plausible claim. *See* Dkt. 127 at 8-9. Relying on the Court’s statement that “the retailers joined the network created by AddShoppers, which caused the plaintiffs to receive unwanted email communications from AddShoppers when they visited the retailers’ websites,” Dkt. 89 at 2, Peet’s argued that Cordero lacked standing because he did “not even allege he received an unwanted email communication from AddShoppers or Peet’s,” Dkt. 127 at 9. Peet’s further argued that Cordero’s allegation that “he had been tracked by at least a dozen companies for several years,” including other companies that were part of the AddShoppers network, “further minimiz[ed] the significance of any supposed information about Mr. Cordero allegedly captured on the Peet’s website.” *Id.*

On November 21, 2024, the Court issued an order granting Plaintiffs’ motion for leave to file the First Amended Complaint. *See* Dkt. 132.

On December 6, 2024, Peet’s and AddShoppers moved to dismiss the First Amended Complaint, focusing primarily on three arguments the Court previously addressed and rejected: (1) the non-California plaintiff lacks standing to assert claims under California statutory law; (2) Plaintiffs lack Article III standing; and (3) Plaintiffs fail to adequately plead their CIPA and CDAFA claims. This opposition follows.

² The Amended Complaint left in several claims previously dismissed by the Court but noted that Plaintiffs were not seeking reconsideration of those claims and instead were including them to preserve appellate rights.

III. ARGUMENT

A. Legal Standards

1. Motion to Dismiss

Defendants move to dismiss under Rules 12(b)(1) and 12(b)(6). When jurisdictional and merits issues are intertwined, disputed facts should not defeat jurisdiction. *Safe Air for Everyone v. Meyer*, 373 F.3d 1035, 1039 (9th Cir. 2004). Under Rule 12(b)(6), the complaint need only contain enough facts that, if true, make the claim plausible. *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009).

2. Law of the Case

The “law of the case” doctrine bars courts from reconsidering issues they have already decided. *See Chavez v. Bank of Am. Corp.*, 2012 WL 1594272, at *4–5 (N.D. Cal. May 4, 2012) (citing *Thomas v. Bible*, 983 F.2d 152, 154 (9th Cir. 1993)). A court must follow its prior decisions on factual or legal issues in all subsequent proceedings unless: (1) substantial new or different evidence is presented; (2) controlling authority changes on the particular issue; or (3) the prior decision was clearly erroneous and would cause manifest injustice. *See id.* at *4 (citing *In re Benny*, 81 F.3d 91, 94 (9th Cir. 1996)).

This doctrine is not substantive law but a practical rule preventing repeated reargument of decided issues. *Id.* at *5 (citing 18 Charles Alan Wright et al., *Federal Practice and Procedure* § 4478, at 790 (1981)). It applies to: (1) issues explicitly decided; (2) matters decided by necessary implications; (3) issues given only summary treatment; and (4) even “cryptic and somewhat ambiguous” rulings. *Id.* (quoting *Hanna Boys Ctr. v. Miller*, 853 F.2d 682, 687 (9th Cir. 1988)). Whether a ruling becomes law of the case depends on whether the court actually decided the issue—not on how thoroughly it explained its reasoning. *Id.* (citing *Christianson v. Colt Indus. Operating Corp.*, 486 U.S. 800, 817 (1988)).

B. Plaintiffs have standing to pursue all their claims.

To establish Article III standing, Plaintiffs must show (1) an injury, (2) that results from

Defendants’ conduct (3) that a court can redress. *Spokeo, Inc. v. Robins*, 578 U.S. 330, 338 (2016). Defendants both challenge the existence of an injury, renewing arguments this Court has already considered and rejected in prior orders.

1. The law of the case doctrine bars re-litigation of these issues.

In its prior motion to dismiss order, the Court held that the plaintiffs adequately alleged Article III standing against both AddShoppers and the retailer defendants. Specifically, the Court explained that misappropriating individuals’ browsing activity across a network of online retailers and using that data to send unsolicited emails constitutes an actionable intrusion on privacy under federal law. Dkt. 89 at 2 (citing *TransUnion LLC v. Ramirez*, 594 U.S. 413, 424-25 (2021); *In re Facebook, Inc. Internet Tracking Litig. (Facebook Tracking)*, 956 F.3d 589, 598 (9th Cir. 2020); *In re Facebook, Inc., Consumer Privacy Litig.*, 402 F. Supp. 3d 767, 784-87 (N.D. Cal. Sept. 2019)). The Court determined that AddShoppers “orchestrated the scheme” and took direct actions that caused harm, “clearly” establishing standing. Dkt. 89 at 2. And the retailer defendants knowingly participated in the scheme by facilitating the collection and use of consumers’ aggregated browsing data, which was enough to confer standing to sue them as well. *Id.*

Defendants’ argument against standing remains the same. They contend Cook (and now Cordero) lack standing because neither “alleges to have provided personal information when visiting Peet’s website. Nor do they allege that Peet’s collected any information that is considered ‘personal’ or ‘private.’” Dkt. 139 at 12; *compare id. and* Dkt. 138 at 13-14 *with* Dkt. 51 at 14 (“Plaintiffs . . . do not allege any facts showing that they disclosed any sensitive information to Peet’s, much less identify any specific personal information either disclosed that implicates a protectable privacy interest”) (cleaned up). Defendants even rely on the same two “session replay” cases. *Compare* Dkt. 139 at 13-16 (citing *Lightoller v. Jetblue Airways, Corp.*, 2023 WL 3963823, at *4-5 (S.D. Cal. June 12, 2023) and *Byars v. Sterling Jewelers, Inc.*, 2023 WL 2996686 (C.D. Cal. Apr. 5, 2023)) *with* Dkt. 51 at 13-14 (citing same). But the Court made clear that those two “cases do not stand for the proposition that a website only causes a privacy injury where it collects

the personal information *itself*. The whole idea of AddShoppers’ scheme is to tie browsing activity on one site with personal information disclosed on another site, obviating the need for the retailers to do it themselves.” Dkt. 89 at 3 n.1.

Defendants offer no new facts or controlling authority to warrant reconsideration of this issue. *See Chavez*, 2012 WL 1594272, at *4. They instead point to *Ingrao v. AddShoppers, Inc.*, 2024 WL 4892514 (E.D. Pa. Nov. 25, 2024), and the Third Circuit cases upon which it relies, which dismissed similar claims for lack of standing. But that Eastern District of Pennsylvania decision is not “a change in *controlling* authority applicable to the particular issue.” *Chavez*, 2012 WL 1594272, at *4 (emphasis added). To the contrary, *Ingrao* does not cite or even acknowledge the Court’s order addressing similar issues, suggesting that the court viewed the standing analysis differently under Third Circuit law. Nor does it address binding Ninth Circuit precedent like *Facebook Tracking*.

Defendants’ assertion that Cordero lacks standing because he did not allege receipt of an email or the capture of sufficiently private information is not new either. Peet’s contested Plaintiffs’ motion to add Cordero as futile for this reason. *See* Dkt. 127 at 8-9. The Court implicitly rejected these arguments when it granted leave to amend the complaint. *See* Dkt. 132. And Defendants provide no basis to revisit that ruling. *See Chavez*, 2012 WL 1594272, at *5 (explaining that law of the case doctrine applies to “matters that were decided by necessary implication in the court’s prior ruling”).

2. Even if not barred, Defendants’ standing arguments are not persuasive.

Even if the law of the case doctrine did not apply here, Defendants’ standing arguments lack merit.

3. Plaintiff Cordero has Article III standing.

Defendants argue that Cordero fails to show a concrete injury because he does not allege that he received an email from AddShoppers or Peet’s—“let alone a ‘barrage’” of them. Dkt. 138 at 13-14. But as the Court already held, the harm that establishes standing isn’t necessarily the

receipt of unsolicited emails—it’s the misappropriation of the internet user’s private browsing data. *See* Dkt. 89 at 2-3 (“The ultimate injury is not merely the dissemination of one unwanted email from one website; it is the aggregation of information about a consumer’s browsing history across thousands of retail sites and the systematic dissemination of emails from the AddShoppers’ network based upon that information.”). The operative complaint adequately pleads that Cordero’s data was misappropriated: it alleges he was tracked by dozens of AddShoppers’ retail partner companies, including Peet’s, for several years. *See* Dkt. 135 (“FAC”) ¶ 63.

At any rate, even if receiving an unwanted email were a prerequisite to standing, the complaint sufficiently alleges that Cordero received one. It states that Cordero specifically requested his data from AddShoppers, and a reasonable inference is that Cordero’s receipt of an email prompted his request. *Id.* After all, Cordero alleges no preexisting relationship with the company, so how else would he know it tracked him? And *as Defendants already know*, that is precisely what happened. *See* Dkt. 121-1 ¶¶ 1-5 (Cordero received his first email via SafeOpt to his Gmail account on June 28, 2024, and subsequently requested his data from AddShoppers, which confirmed he had been tracked while visiting Peet’s website).

Moreover, Defendants’ attempts to downplay the information collected as mere “innocuous” metadata—like the “exact dates and times” that Cordero visited websites—mischaracterizes the allegations in the complaint. Dkt. 138 at 13-14; *see also* Dkt. 139 at 15. The complaint alleges that AddShoppers’ tracking code captures detailed browsing data, including referrer URLs and specific products viewed. *See* FAC ¶¶ 35, 37. In fact, AddShoppers’ entire business model relies on capturing users’ interactions with specific products and content. So although AddShoppers only provided metadata in response to Cordero’s pre-filing data request,³

³ AddShoppers’ practice of making incomplete data disclosures to California residents very likely violates the CCPA. *See* Cal. Civ. Code § 1798.110 (upon request, businesses must disclose to California residents: (1) the categories of personal information it has collected about that consumer; (2) the categories of sources from which the personal information is collected; (3) the business or commercial purpose for collecting, selling, or sharing personal information; (4) the

it collected far more data about his browsing activities. AddShoppers cannot rely on its deficient disclosures or an overly narrow reading of the complaint to minimize the full scope of its data collection practices prior to discovery.

4. Plaintiff Lineberry has Article III standing.

AddShoppers next advances a novel but baseless argument that Plaintiff Abby Lineberry lacks a protectable privacy interest in her “work-related browsing history.” Dkt. 138 at 15-16. This argument fails for several reasons.

To start, AddShoppers’ premise rests on an illogical reading of the complaint. AddShoppers assumes, without basis, that Lineberry was tracked only on a work computer while conducting purely work-related browsing. In reality, Lineberry entered the AddShoppers network when an unknown retailer captured her *personal* email address. *See* FAC ¶ 55. This fact alone defeats AddShoppers’ claim that the tracking occurred solely in her professional capacity. While the complaint notes that Lineberry *discovered* the tracking when “her *work*-related browsing history was . . . emailed to her *personal* email address by a company she never provided it to,” this merely describes how she learned about the surveillance. *Id.* ¶ 56.

But more fundamentally, AddShoppers’ argument misses a basic privacy principle: the nature of browsing activity—whether personal or professional—does not diminish the privacy interest in preventing unauthorized interception. For example, if someone’s phone is wiretapped, the wiretapper’s liability does not turn on whether the intercepted calls were personal or work-related. The violation stems from the unauthorized capture itself. *See Facebook Tracking*, 956 F.3d at 607 (“CIPA prohibits any person from using electronic means to ‘learn the contents or meaning’ of any ‘communication’ ‘without consent’ or in an ‘unauthorized manner.’”) (quoting Cal. Penal Code. § 631(a)).

AddShoppers undermines its own contrary position by arguing that “it is common sense

categories of third parties to whom the business discloses personal information; and (5) the specific pieces of personal information it has collected about that consumer).

that an employer may monitor the online activity of their employees who are working on company-owned computers.” Dkt. 138 at 16. Even if employees expect workplace monitoring by their employer, that expectation does not extend to surveillance by *unknown third parties* like AddShoppers. Tellingly, AddShoppers can only muster support for its position by citing inapposite criminal cases about whether employer monitoring violates Fourth Amendment rights. *See* Dkt. 138 at 15-16. Even those cases, however, require employers to properly disclose their monitoring policies.⁴

C. Plaintiffs have sufficiently pleaded their statutory claims.

The remaining arguments raised by Defendants have already been argued and decided.

1. The Court has already rejected Peet’s argument that non-California representatives cannot assert claims against California companies.

Disregarding the Court’s prior decisions, Peet’s again argues that Cook fails to state a CIPA or CDAFA claim because he hasn’t alleged an interception in California. *Compare* Dkt. 139 at 19 with Dkt. 51 at 16 (“[T]he only reasonable inference is that Plaintiffs Cook and Dessart interacted with the Retail Defendants’ websites while in their home states. Indeed, Plaintiffs do not even allege any interception occurred in California.”). Plaintiffs previously defeated this argument by citing clear precedent that at the pleading stage non-California plaintiffs can pursue claims against California companies under these statutes. *See* Dkt. 60 at 29-30 (citing *Carrese v. Yes Online Inc.*, 2016 WL 6069198, at *4 (C.D. Cal. Oct. 13, 2016) (“CIPA applies to the action, to the extent the Complaint asserts CIPA claims against a California defendant alleged for alleged conduct that

⁴ *See, e.g., United States v. Greiner*, 235 F. App’x 541, 542 (9th Cir. 2007) (“The warning banner confronting Greiner every time he logged onto his computer gave him ample reason to be aware that his stored files and internet usage were subject to monitoring by his employer and disclosure to law enforcement personnel.”); *United States v. Caputo*, 2019 WL 5788305, at *4 (D. Or. Nov. 6, 2019) (“[A]ny expectation of privacy in Defendant’s work email was objectively unreasonable under the military’s computer-use policies in effect at his workplace. . . .”); *see also United States v. Heckenkamp*, 482 F.3d 1142, 1146-47 (9th Cir. 2007) (holding that a public university’s limited monitoring policy did not diminish a student’s reasonable expectation of privacy in files on his personal computer connected to the university network).

occurred in California.”) (collecting cases); *Balanzar v. Fidelity Brokerage Servs., LLC*, 654 F. Supp. 3d 1075, 1086 (S.D. Cal. 2023) (“It is a reasonable inference for the Court to make that any phone call Plaintiff makes to any one of these locations in California would involve the use of the MyVoice system in the state of California.”)). The Court found Peet’s argument “too weak or undeveloped to merit a response.” Dkt. 89 at 5. Peet’s spent no more time developing it now.⁵

2. The Court has already decided that Plaintiffs sufficiently allege the elements of CIPA.

Under CIPA, Plaintiffs must show AddShoppers “(1) willfully (2) and without Plaintiffs’ consent (3) read or attempted to read or learn the contents of their communications (4) while the communications were being sent from, received in, or in transit or passing over any wire, line or cable in California.” *Torres v. Prudential Fin., Inc.*, 2024 WL 4894289, at *4 (N.D. Cal. Nov. 26, 2024). Peet’s, in turn, is liable for aiding and abetting AddShoppers’ violation. *Id.* In their initial motions to dismiss, Defendants challenged two elements: (1) whether communications were intercepted “in transit” in California; and (2) whether confidential content was captured. *See* Dkt. No. 50 at 17 (arguing the “in transit” element was not met); Dkt. No. 51 at 21-22 (asserting that the CIPA claim failed because plaintiffs did not disclose confidential information during their website visits). Neither has merit this round.

Plaintiffs thoroughly rebutted these arguments by detailing AddShoppers’ real-time interception of communications—allegations far more specific than the conclusory claims courts typically reject under CIPA. *See* Dkt. No. 60 at 31-32; *see also Hazel v. Prudential Fin., Inc.*, 2023 WL 3933073, at *3 (N.D. Cal. June 9, 2023) (distinguishing between conclusory and sufficient allegations of “in transit” element). Plaintiffs also established that URLs constitute protected information because they reveal users’ personal interests and browsing habits. *See* Dkt. No. 60 at 33 (citing *Facebook Tracking*, 956 F.3d at 605 (noting that URLs divulge “a user’s personal

⁵ Peet’s assertion that the addition of Cordero to the complaint constitutes an “admi[ssion]” of Plaintiff Cook’s inability to pursue California statutory claims is both speculative and irrelevant to the legal standards governing the analysis. Dkt. 139 at 11.

interests, queries, and habits on third-party websites operating outside of Facebook’s platform”)).

The Court agreed with Plaintiffs, finding they “sufficiently allege[d] that the communications were intercepted ‘in transit’ within the meaning of § 631(a).” Dkt. 89 at 5. It emphasized that the complaint went beyond mere statutory recitation by detailing “how AddShoppers’s cookies intercept the information in real time” and citing AddShoppers’ own statements about real-time transmission. *Id.*

Yet Defendants resurrect their rejected arguments here. Peet’s revives its claims about California interception, *compare* Dkt. No. 51 at 21-22 *with* Dkt. No. 139 at 19, and AddShoppers renews its privacy argument about the contents of the communications, *compare* Dkt. No. 51 at 21-22 *with* Dkt. No. 138 at 19-20. These arguments remain unpersuasive and contradict the Court’s prior ruling. Plaintiffs have adequately alleged real-time interception, protected URL content, and conduct within § 631(a)’s scope. *See Mata v. Zillow Grp., Inc.*, 2024 WL 5161955, at *5 (S.D. Cal. Dec. 18, 2024) (finding tracking pixel collected content of communications in real time); *Yoon v. Meta Platforms, Inc.*, 2024 WL 5264041, at *5 (N.D. Cal. Dec. 30, 2024) (same). Defendants’ arguments about Cordero are similarly misguided in suggesting that AddShoppers merely tracked visit timing and locations. As explained above, these arguments ignore the complaint’s allegations about AddShoppers capturing referrer URLs and detailed product viewing information.⁶

3. Defendants’ recycled CDAFA arguments should again be rejected.

AddShoppers challenges Plaintiffs’ statutory standing under CDAFA, focusing on the benefit of the bargain allegations.⁷ Dkt. 138 at 16-17. This challenge, however, misses the mark because Plaintiffs’ damages theory does not rely on benefit of the bargain damages.

Both Defendants also rehash their previous argument that Plaintiffs fail to allege sufficient

⁶ AddShoppers’ own marketing materials acknowledge as much, noting that AddShoppers can send shoppers “the *products or content* they were looking at directly to their inbox.” FAC ¶ 37 (emphasis added).

⁷ AddShoppers also challenges Plaintiffs’ statutory standing under the UCL, *see* Dkt. 138 at 16-17, but Plaintiffs are no longer pursuing their UCL claim and thus do not oppose dismissal of that claim, *see* Dkts. 136, 144.

economic damages under CDAFA. *Compare* Dkt. 50 at 19 *with* Dkt. 138 at 17 (“CDAFA only allows for recovery of specific type of damage, which has not been alleged here.”) (emphasis omitted); *see also* Dkt. 139 at 21 (“Plaintiffs Cook and Cordero . . . fail to allege any damage or loss as required to bring a claim under CDAFA”). In opposing their first motions to dismiss, Plaintiffs cited *Brown*, 685 F. Supp. 3d at 940, which held on summary judgment that misappropriated browsing histories can create economic injury under CDAFA based on the defendant’s own valuation of such data. *See* Dkt. 60 at 34. *Brown* recognized under *Facebook Tracking*, “plaintiffs can state an economic injury for their misappropriated data.” *Id.* at 960. Plaintiffs’ allegations fit squarely within this framework. AddShoppers misappropriated Plaintiffs’ personal information for “economic and commercial advantage.” Compl. ¶ 128; *see also* FAC ¶ 119. And because AddShoppers claims a “license” over their information, Plaintiffs are entitled to recover the value of the unauthorized access, measurable through damages theories akin to intellectual property remedies (like reasonable royalties from infringers). FAC ¶ 68.

The Court has already sustained Plaintiffs’ CDAFA claim after considering these same arguments. *See* Dkt. 83 at 6. Defendants’ attempt to relitigate this issue ignores both Ninth Circuit authority and the Court’s prior ruling. Plaintiffs have adequately alleged economic harm under CDAFA based on the financial value of their misappropriated data, including detailed browsing histories and product interactions. *See Frasco v. Flo Health, Inc.*, 2024 WL 4280933, at *3 (N.D. Cal. Sept. 23, 2024) (finding evidence that misappropriated information “carried financial value” sufficient to establish damage or loss under CDAFA); *see also Rodriguez v. Google LLC*, 2024 WL 38302, at *6 (N.D. Cal. Jan. 3, 2024) (certifying CDAFA class based on classwide evidence of data’s financial value and defendants’ profits). The Court should again reject Defendants’ recycled arguments.

IV. CONCLUSION

The Court should reject Defendants’ repeated attempts to relitigate issues already decided and deny their motions in full.

Dated: January 7, 2025

Respectfully submitted,

/s/ J. Austin Moore

Norman E. Siegel (*pro hac vice*)

J. Austin Moore (*pro hac vice*)

Kasey Youngentob (*pro hac vice*)

STUEVE SIEGEL HANSON LLP

460 Nichols Road, Suite 200

Kansas City, Missouri 64112

(816) 714-7100 (tel.)

siegel@stuevesiegel.com

moore@stuevesiegel.com

youngentob@stuevesiegel.com

David M. Berger (SBN 277526)

GIBBS LAW GROUP LLP

1111 Broadway, Suite 2100

Oakland, California 94607

Telephone: (510) 350-9713

Facsimile: (510) 350-9701

dmb@classlawgroup.com